PREDICT Red Team Assessment

its purpose, methods, and summary findings

Kevin D. Robbins

Sandia National Laboratories
Information Operations Red Team and Assessments
Critical Infrastructure Systems

27 September 2005

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Assessment Purpose

the PREDICT Program

Essentially, the PREDICT Program brokers relationships between *researchers*, *data hosts*, and *data providers* to

- advance network security research and development by
- facilitating the sharing of datasets for test and evaluation of
- maturing network security technologies.

These datasets are individually and collectively sensitive;
access to these datasets must be limited to those with legitimate need.

Assessment Purpose

and why involve a red team?

To fulfill its purpose, the PREDICT Program must

- provide secure brokerage services, currently provided by the PREDICT Portal,
- build trust and confidence among PREDICT program participants, especially among data providers, and
- enforce memoranda of agreement.

Sandia National Laboratories' red team provides the adversarial view to provide feedback needed to meet these goals.

The red team offers an objective analysis to assist the development team.

Red Teams

and their common uses

Red teams are used for a number of purposes including

- design assurance – to improve the design and implementation of a system throughout its lifecycle,
- oppositional force – to generate probable adversary observables and to train blue forces by impersonating constrained, reproducible adversaries,
- tactical analysis – to rapidly assess scenarios from a technical and adversarial perspective,
- experimentation – to explore system response or to make decisions through the stimulus of an adversary, and
- demonstration – to validate an attack plan on real systems and under operational constraints.

Information Operations Red Team and Assessments

five dimensions of IORTA^{TM}assessments

IORTA^{TM}assessments are easily adapted along five dimensions:

- assessment type – risk, information technology management, information technology security, red team, and opositional force red team;
- assessment approach – tactical red team analysis cell, whiteboard, quick-look, quick-look plus, full, experiment;
- process and technique – internal, external, team composition, and training;
- measurement – metrics built into processes, R&D;
- characterization views and analysis – physical, logical, temporal, consequence, system, and others.

Information Design Assurance Red Team

the IDART^{TM}Methodology

The IDART^{TM}Methodology provides independent assessments

- performed from an adversarial point of view
- that are consequence-based and system oriented.

The methodology provides structured team processes that help

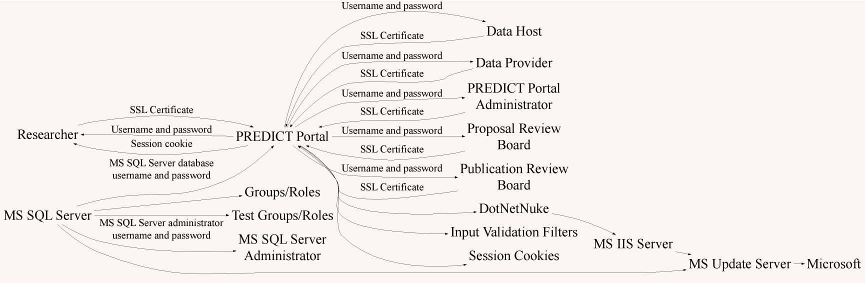
- build thorough understanding of complex systems-of-systems,
- generate creative and unexpected attack ideas, and
- focus analysis effort to maximize usefulness of asssessments.

System characterization builds graphical system views to

- clarify systems-of-systems understanding and to
- support attack enumeration.

A System Characterization Example

a trust diagram



Username and password
SSL Certificate
Data Host
Username and password
SSL Certificate
Data Provider
Username and password
SSL Certificate
PREDICT Portal Administrator
SSL Certificate
Username and password
Session cookie
Researcher
PREDICT Portal
Username and password
SSL Certificate
Proposal Review Board
MS SQL Server database username and password
Username and password
SSL Certificate
Publication Review Board
Groups/Roles
MS SQL Server
Test Groups/Roles
MS SQL Server administrator username and password
MS SQL Server Administrator
DotNetNuke
Input Validation Filters
MS IIS Server
Session Cookies
MS Update Server
Microsoft

Trust diagrams show

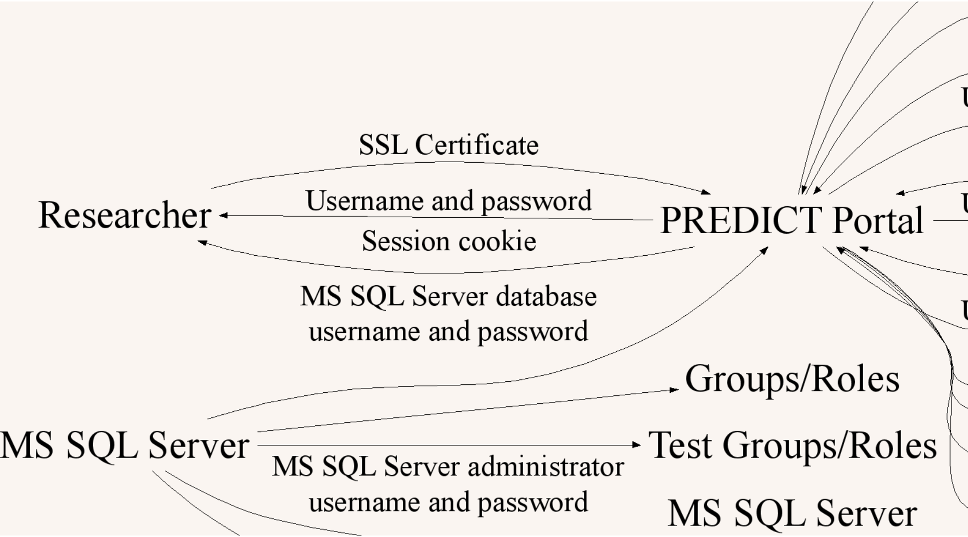
- who trusts whom and
- on what basis.

PREDICT Portal trusts Researcher on the basis of

- username, password,
- and session cookie.

A System Characterization Example

a trust diagram



Researcher

PREDICT Portal

SSL Certificate

Username and password

Session cookie

MS SQL Server database
username and password

Groups/Roles

MS SQL Server

Test Groups/Roles

MS SQL Server administrator
username and password

MS SQL Server

PREDICT Red Team Assessment

its methods and scope

The PREDICT Red Team Assessment applied the

- IDART^{TM}Methodology to
- PREDICT policies, procedures, and processes defined and implemented
- by the PREDICT Portal (www.predict.org) and to
- the PREDICT Portal itself.

Assessment scope did not include shared infrastructure
on which the PREDICT Portal is currently built;
nor did it include assessment of data host security.

Summary Findings

recurring security themes

Many of the PREDICT Program policies, procedures, and processes are defined, implemented, and enforced through the PREDICT Portal.

The PREDICT Portal implements rich functionality on an Internet host and user input validation must be carefully maintained to prevent cross-site scripting and SQL Injection exploits.

Other recurring security issues include

- authentication of parties brokered by the PREDICT Program and
- validation of dataset transfers among program participants.